UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/759,402	01/12/2001	George Cybenko	389522	1647

30955	7590	10/23/2006

LATHROP & GAGE LC
4845 PEARL EAST CIRCLE
SUITE 300
BOULDER, CO 80301

EXAMINER
MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _16 August 2006_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-16_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-16_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _12 January 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some *   c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 16 August 2006.

2. Claims 1-16 are pending in the application.

3. Claims 1-16 have been rejected.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 16 August 2006 has been entered.

Response to Arguments

5. Applicant's arguments with respect to claims 1-16 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Independent claim 1 recites the limitation "wherein computations and data associated with the program and data string are unintelligible and useless at the host computer". The examiner asserts that both the terms "unintelligible" and "useless" are relative and indefinite terms.

Independent claim 15 recites the limitation "a secured computer network for executing encrypted computer programs at a remote host computer without sharing intelligible or otherwise useful program code" and "the host computer having substantially no intelligible or otherwise useful program code". The examiner asserts that both the terms "unintelligible" and "useless" are relative and indefinite terms.

7. Claims 15 and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite in that it fails to point out what is included or excluded by the claim language. This claim is an omnibus type claim.

Claim 15 recites the l limitation "the host computer having substantially no intelligible or otherwise useful program code". The term "substantially" renders the claim an omnibus type claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Silverstein et al

U.S. Patent No. 5,677,696.

As to claim 1, Silverstein et al discloses a method for encrypting programs for encrypted

execution on a network having a remote host computer, comprising the steps of:

encrypting a program as a unitary matrix with n rows and n columns

[column 4, lines 32-63];

encrypting an input data string to the program as a vector of length n,

wherein execution of the program on the input data string is realized by matrix

multiplication of the unitary matrix with the vector [column 9 line 51 to column

10 line 49];

loading the encrypted program and the encrypted data string on the host

computer [column 9 line 51 to column 10 line 49];

executing the encrypted program, using the encrypted data string, on the

host computer [column 9 line 51 to column 10 line 49];

communicating results from the host computer to the network [column 9

line 51 to column 10 line 49]; and

decoding the results into output representative of executing the program

with the data string, wherein computations and data associated with the program

and data string are unintelligible and useless at the host computer [column 9 line

51 to column 10 line 49].

As to claim 2, Silverstein et al discloses that the step of encrypting a program comprises

converting the program to a unitary matrix multiplication [column 9 line 51 to column 10 line

49].

As to claim 3, Silverstein et al discloses that the step of converting the program

comprises converting the program to a unitary matrix multiplication U such that $U \ \varepsilon \ U_n$ for some

integer n, where U_n represents a group of unitary matrices of size n [column 4, lines 32-63].

As to claim 4, Silverstein et al discloses that the step of encrypting the program

comprises generating two independent identically distributed unitary matrices X, Y from the

uniform probability distribution over U_n determined by the Haar distribution [column 9 line 51 to

column 10 line 49].

As to claim 5, Silverstein et al discloses that the step of encrypting a program comprises

the steps of computing U' as XUY* and communicating U' to the remote host computer over the

network [column 8, lines 9-46].

As to claim 6, Silverstein et al discloses that the step of encrypting the input data string

comprises converting the input data string to a vector b [column 8, lines 9-46].

As to claim 7, Silverstein et al discloses that the step of encrypting comprises the steps of

computing b' as Yb and communicating b' to the remote host over the network [column 8, lines

9-46].

As to claim 8, Silverstein et al discloses that the step of executing the encrypted program, using the encrypted data string, on the: host computer comprises the steps of computing the product of XUY* and Yb and communicating results to the network [column 9, lines 24-46].

As to claim 9, Silverstein et al discloses that the step of decoding the results into output comprises computing X*XUb, external of the host computer, to determine the multiplication of Ub as desired output of the programs wherein XUY* and Yb is (XUb) and X*XUb is obtained by matrix multiplication X*(XUb) [column 9, lines 24-46].

As to claim 10, Silverstein et al discloses the step of decoding comprises decrypting at a control computer connected to the network and the host computer [column 9, lines 24-46].

As to claim 11, Silverstein et al suggests that the network comprises the Internet [column 3, lines 27-42].

As to claim 12, Silverstein et al suggests that the network comprises a virtual private network [column 3, lines 27-42].

As to claim 13, Silverstein et al suggests that the network comprises a local area network (LAN) [column 3, lines 27-42].

As to claim 14, Silverstein et al discloses embedding one or more constants into the input data string or program, prior to encrypting, to detect incorrect execution or data tampering [column 16 line 1 to column 17 line 67].

As to claim 15, Silverstein et al discloses a secured computer network for executing

encrypted computer programs at a remote host computer without sharing intelligible or otherwise

useful program code, computations or data associated with execution, comprising:

a control computer for encrypting a program as a unitary matrix with n

rows and n columns and for encrypting an input data string to the programs as a

vector of length n, wherein execution of the program on the input data string is

realized by matrix multiplication of the unitary matrix with the vecto [column 4,

lines 32-63]r; and

a host computer, in network with the control computer, for loading the

encrypted program and the encrypted data string, the host computer executing the

encrypted program, using the encrypted data string, and communicating results to

the control computer decoding, the host computer having substantially no

intelligible or otherwise useful program code, computations or data associated

with execution of the encrypted program [column 9 line 51 to column 10 line 49].

As to claim 16, Silverstein et al discloses that the control computer embeds one or more

constants into the unitary matrix or data string, wherein the results from the host computer

indicate tampering or incorrect execution of the encrypted program [column 9 line 51 to column

10 line 49].

Conclusion

9.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy
October 20, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100